Statewide Information Technology Standards
Version No. 1

Office of the Governor
State Chief Information Officer

SECURITY

Chapter 9 – Dealing with Premises Related Considerations

Scope: These standards apply to all public agencies, their agents or designees subject to Article 3D of Chapter 147, “State Information Technology Services.”

Statutory Authority: G.S. §147-33.110

Section 01 Premises Security

090101 Preparing Premises to Site Computers and Data Centers

Purpose: To protect equipment through secure site selection and preparation.

STANDARD

Agencies shall carefully evaluate sites and facilities that will house information technology equipment to identify and implement suitable controls to protect hardware from environmental threats, physical intrusion and other hazards.

GUIDELINES

When evaluating or preparing sites and locations for hardware installation, agencies should consider the following:

- Sites and locations for installation of information technology equipment should be carefully selected because of the difficulty of relocating hardware once it is in place.
- Security threats may expand from neighboring premises or adjacent properties.
- Requirements for size and location will vary according to the amount of hardware being housed.
- Physical security measures adopted should reflect the:
  - □ Value of the hardware.
  - □ Sensitivity of the system’s data.
  - □ Required level of availability or fault tolerance.
- Risk assessments may reveal that security controls are needed for natural, structural and human threats such as.
  - □ Explosion.

- ❑ Fire.
- ❑ Smoke.
- ❑ Water (or a failure to supply water).
- ❑ Chemicals.
- ❑ Wind.
- ❑ Seismic activity.
- ❑ Dust.
- ❑ Vibration.
- ❑ Electromagnetic radiation.
- ❑ Electrical supply interference.

ISO 17799: 2005 References
9.2.1 Equipment siting and protection

090102 Securing Physical Protection of Computer Premises

Purpose: To protect information assets via physical security.

STANDARD

Each agency shall safeguard sites, buildings and locations housing its information technology assets.

GUIDELINES

Business operations, business continuity plans and applicable contracts should ensure that natural, structural and human threats have been accurately assessed and that controls are employed to minimize unauthorized physical entry to sites, buildings and locations housing information technology assets.

Security measures that agencies should consider implementing include, but are not limited to, the following:

- Clearly defined, layered security perimeters to establish multiple barriers:
  - ❑ Walls (of solid construction and extending from real ceiling to real floor where necessary).
  - ❑ Card-controlled gates and doors.
  - ❑ Bars, alarms, locks, etc.
  - ❑ Bollards.
  - ❑ Lighting controls.
  - ❑ Video cameras and intrusion security system.
  - ❑ Staffed reception desk.
- Equipping all fire doors on a security perimeter with alarms as well as devices that close and lock the doors automatic.

RELATED INFORMATION

Standard 020103	Securing Unattended Workstations
Standard 050101 Hardware	Specifying Information Security Requirements for New
Standard 090101	Preparing Premises to Site Computers
Standard 090103	Ensuring Suitable Environmental Conditions

ISO 17799: 2005 References
9.1.1 Physical security perimeter

090103 Ensuring Suitable Environmental Conditions

Purpose: To ensure that environmental conditions are suitable for State agency computing resources.

STANDARD

When locating computers and other information technology assets, agencies shall implement appropriate controls to protect the assets from environmental threats, such as fire, flooding and extreme temperatures.

GUIDELINES

Agencies should consider the following information security issues when minimizing the risk of environmental threats:

- Exposed vulnerabilities to environmental risks could hinder or make it impossible for the agency to continue business operations in the event of:
  - ❑ Fire or smoke damage.
  - ❑ Flooding (pipes bursting, fire suppression system or other overhead water conduits malfunctioning, etc.)
  - ❑ Heating, ventilation or air conditioning (HVAC) failures.
  - ❑ Dust or other contaminants.
- Relevant health and safety standards.
- Threats that may expand from neighboring premises.

RELATED INFORMATION

Standard 090102	Securing Physical Protection of Computer Premises

ISO 17799: 2005 References
9.1.3 Securing offices, rooms, and facilities

090104 Physical Access Control to Secure Areas

Purpose: To protect computer equipment by controlling physical access.

STANDARD

Agencies shall protect their computing facilities, locations and rooms from unauthorized access with appropriate physical access controls.

GUIDELINES

Agencies should control the number of people who have physical access to areas housing computer equipment to reduce the threats of theft, vandalism and unauthorized system access.

When implementing physical access controls, agencies should consider the following measures to control and restrict access:

- The access control system should address the following categories of personnel, each with different access needs:
  - ❑ System operators and administrators who regularly work in the computer area.
  - ❑ Technical support staff and maintenance engineers who require periodic access to the computer area.
  - ❑ Other staff who rarely need access to the area.
- Physical access authentication controls should include some form of visible identification such as an ID badge.
- An audit trail of physical access to the computer area should be maintained.
- Visitors to the computer area require additional controls, including the following.
  - ❑ Access should be restricted to those having specific, authorized purposes for visiting the computer area.
  - ❑ Instructions should be issued to visitors explaining security requirements and emergency procedures.
  - ❑ Entry and exit dates and times should be logged.
  - ❑ Visitors should wear visible identification that clearly draws attention to their restricted status.
  - ❑ Visitors should be escorted.

RELATED INFORMATION

Standard 090101	Preparing Premises to Site Computers
Standard 090105	Challenging Strangers on Agency Premises

ISO 17799: 2005 References
9.1.2 Physical entry controls

090105 Challenging Strangers on Agency Premises

Purpose: To increase the security of areas housing information technology equipment.

STANDARD

Each agency shall educate employees to appropriately challenge strangers in areas containing information technology equipment to verify the stranger's authority to be in the controlled area. Where appropriate, employees and visitors shall be properly badged and escorted at all times. Where entrance to an area requires a badge or a similar controlled-access method, authorized individuals shall not allow unauthorized individuals to follow them into the controlled-access area.

ISO 17799: 2005 References
9.1.3 Securing offices, rooms, and facilities

090106 High Security Locations

Purpose: To protect information and assets in high security locations.

STANDARD

Locations that contain confidential information shall be designed and secured in accordance to the information being protected.

Cameras, video recorders and handheld devices (cell phones, PDAs, pocket PCs), shall be restricted from high security locations to protect the information being stored.

ISO 17799: 2005 References
9.1.5 Working in secure areas

090107 Delivery and Loading Areas

Purpose: To protect information and assets in loading areas.

STANDARD

Access to loading docks and warehouses shall be restricted to authorized personnel. Items that are received via loading areas shall be signed for and inspected for hazardous materials before distributed for use.

ISO 17799: 2005 References
9.1.6 Public access, delivery, and loading areas

090108 Duress Alarm

Purpose: To protect personnel and confidential information using alarms.

STANDARD

Duress alarms shall be used in areas where the safety of personnel is a concern. Alarms shall be provisioned to alert others such as staff, the police department, the fire department, etc.

ISO 17799: 2005 References
9.1.5 Working in secure areas

090109 Environmental and Other External Threats

Purpose: To protect personnel and confidential information from threats.

STANDARD

Work locations shall protect staff, information and business assets from environmental and external threats.

GUIDELINES

Agencies should conduct a risk assessment to calculate perceived risks and the total costs involved to mitigate threats to acceptable levels.

ISO 17799: 2005 References
9.1.4 Protecting against external and environmental threats

Section 02 Data Stores

090201 Managing On-Site Data Stores

Purpose: To protect confidential information maintained in on-site data stores.

STANDARD

Agencies shall ensure that on-site data storage locations have adequate access controls to minimize the risk of data loss or damage. Each agency shall maintain duplicate copies of critical data on removable media in data stores.

GUIDELINES

Agencies should consider the following information security issues when planning or implementing on-site data stores:

- The survivability of the data store in the face of man-made or natural disasters.
- The need for periodic testing of backup and restore procedures to verify strengths and identify areas for improvement.
- The importance of maintaining a low profile for the facility or its information-processing functions.

ISO 17799: 2005 References
9.1.2 Physical entry controls
9.1.3 Securing offices, rooms, and facilities

090202 Managing Remote Data Stores

Purpose: To protect confidential information that is stored remotely.

STANDARD

Agencies shall ensure that remote data storage locations have adequate access controls to minimize the risk of data loss or damage. Agencies shall address the following security issues when choosing a location for a remote data store:

- If the agency does not have direct control over the remote location, the agency shall enter into a contract with the owner of the remote location that stipulates the access controls and protection the owner must implement.
- The remote data store contract shall also include the following:
  - ❑ The perimeter security and physical access controls to the site and to the agency's individual data store.
  - ❑ Design requirements for secure data storage (i.e., fire suppression and detection equipment, heating, ventilation, and air conditioning [HVAC], measures to prevent water damage, etc.).
  - ❑ Transportation of removable media to and from the agency.

GUIDELINES

Agencies may wish to consider both direction and distance when choosing a remote data store location. The distance between the main computing site and the remote site should be great enough to minimize the risk of both facilities being affected by the same disaster (e.g., fire, hurricane, explosion, etc.).

ISO 17799: 2005 References

9.1.1	Physical security perimeter
9.1.2	Physical entry controls
9.1.3	Securing offices, rooms, and facilities

Section 03 Other Premises Issues

090301 Electronic Eavesdropping

Purpose: To prevent unauthorized access to information and to State information technology systems through eavesdropping on electronic signals, specifically IEEE 802.11 wireless communications with the North Carolina State Network or its components.

STANDARD

All Institutes for Electrical and Electronics Engineers (IEEE) 802.11 wireless network access points on the State Network shall have the following security measures implemented to prevent electronic eavesdropping by unauthorized personnel:

- Physical access
  - ❑ All network access points (APs) and related equipment such as base stations and cabling supporting wireless networks shall be secured with locking mechanisms or kept in an area where access is restricted to authorized personnel.
  - ❑ The reset function on APs shall be used only by and accessible only to authorized personnel.
- Network access
  - ❑ APs shall be segmented from an agency's internal wired local area network (LAN) using a gateway device.
  - ❑ The Service Set Identifier (SSID) shall be changed from the default value.
  - ❑ The SSID shall not contain characters that indicate the location of the wireless LAN (WLAN) access point, the name of the agency, or any other identifying name.
  - ❑ The SSID broadcast function shall be disabled, except where technology does not permit. In cases in which the broadcast SSID function cannot be disabled, the network administrator shall notify the agency security liaison in writing.
  - ❑ A device must be prevented from connecting to a wireless network unless it can provide the correct SSID.
- System access
  - ❑ Every device used to access the State Network over an IEEE 802.11 wireless connection shall have a personal firewall (software or hardware) and up-to-date antivirus software. Devices incapable of running antivirus or personal firewall software, such as personal digital assistants (PDAs) and radio frequency identification (RFID) tags, shall be exempt from this requirement.
  - ❑ All access points shall require a password to access its administrative features. This password shall be stored and transmitted in an encrypted format.
  - ❑ The ad hoc mode for IEEE 802.11, also referred to as peer-to-peer mode or Independent Basic Service Set (IBSS), shall be disabled. The ad hoc mode shall be allowed in the narrow situation in which an emergency temporary network is required.
  - ❑ Every device used to access the State Network over an 802.11 wireless connection shall, when not in use for short periods of time, be locked (via operating system safeguard features) and shall be turned off when not in use for extended periods of time, unless the device is designed to provide or utilize continuous network connectivity. (Such items might include wireless cameras, RFID tag readers and other portable wireless devices.)
  - ❑ If supported, auditing features on wireless devices shall be enabled and the audits reviewed periodically by designated staff.

- Authentication
  - ❑ All wireless access to the State Network via an 802.11 wireless network shall be authenticated by requiring the user to supply the appropriate credentials. Additional authentication shall also be performed through such technologies as Secure Sockets Layer (SSL), Secure Shell (SSH), or Virtual Private Network (VPN) when a LAN is extended or a wide area network (WAN) is created using 802.11 wireless technology.
  - ❑ 802.11x credentials for individual users shall be deactivated in accordance with an agency's user management policy or within twenty-four (24) hours of notification of a status change (for example, employee termination or change in job function).
- Encryption
  - ❑ Depending on the type of information traversing a wireless LAN, encryption is required at varying levels as noted in the section below on wireless LAN defense-in-depth architecture. At a minimum, public information requires Wi-Fi Protected Access (WPA) encryption and confidential data require 802.11i (WPA2)-compliant Advanced Encryption Standard (AES) encryption. End-to-end encryption is highly recommended for the confidential data classification.
  - ❑ When WPA2 is used, AES encryption shall be enabled and shall be no less than 128 bits.
  - ❑ When WPA is used, the highest level of encryption supported on the device shall be enabled.
  - ❑ WPA encryption must use Temporal Key Integrity Protocol (TKIP) or other IEEE- or National Institute of Standards and Technology (NIST)-approved key exchange mechanism.
  - ❑ WPA2 (802.11i) encryption must use CCMP or other IEEE- or NIST-approved key exchange mechanism.
  - ❑ Wired Equivalent Privacy (WEP) shall not be relied upon for wireless security.
  - ❑ When end-to-end encryption is required across both an 802.11 wireless and a wired network, then in addition to WPA2 (802.11i), data transmitted between any wireless devices shall be encrypted using a proven encryption protocol that ensures confidentiality. Such protocols include SSL, SSH, IP Security (IPSec) and VPN tunnels.
  - ❑ Pre-shared keys shall be strong in nature, randomly generated and redistributed to users at least quarterly to protect against unauthorized shared-key distribution or other possible key exposure situations. Pre-shared keys sent by email shall be encrypted.
- Wireless system management
  - ❑ Simple Network Management Protocol (SNMP) shall be disabled if not required for network management purposes.

  - If required for network management purposes, SNMP shall be read-only, with appropriate access controls that prohibit wireless devices from requesting and retrieving information.
  - If SNMP is required for dynamic reconfiguration of access points to address AP failures and rogue AP's, the SNMP protocol used shall adhere to SNMP version 3 standards and take place only on the wired side of the network.
  - Predefined community strings such as *public* and *private* shall be removed.
  - The latest version of SNMP supported by both device and management stations shall be implemented and support for earlier versions of SNMP disabled.
  - IEEE 802.11 wireless devices shall not be used to manage other systems on the network except in temporary, ad hoc, emergency situations or by use of end-to-end encryption with authentication.

- WAN connections
  - Authentication shall be performed when point-to-point wireless access points are used between routers to replace traditional common carrier lines.
- Audit
  - Agencies using 802.11 wireless LANs must enable rogue access point detection in the management software of the WLAN, if available, and search their sites using wireless sniffers at least monthly to ensure that only authorized wireless access points are in place. This type of audit is also recommended for sites not using wireless technologies to detect rogue access points and end-user-installed free-agent access points.
  - The management system shall monitor the airspace in and around agency facilities for unauthorized access points and ad hoc networks. If unauthorized devices are found, the management system shall allow personnel to take appropriate steps toward containment.
- Wireless LAN defense-in-depth architecture

Access	Isolated WLAN	Credential Management	Broadcast SSID	Rotating SSID/PSK	MAC ACL	WPA w/ Strong PSK	802.11i w/ Strong PSK	802.11i w/ 802.1x*	Encryption	VPN	Personal Firewall + AV **
Public Citizens											
Open WLAN for On-Site Citizen Use	Firewall***	SSID	No	Required	—	—	—	—	—	—	—
State Employees/Contractors											
Public Information	WLAN Gateway	PSK	No	Required	Optional	Minimum	Recommended	—	Required	—	Required
Confidential Information	WLAN Gateway	802.1x	No	—	Optional	—	—	Minimum	Required	Recommended	Required
Remote Access											
Access into Agency Network from Wi-Fi Hot Spot by State Employees/Contractors	—	VPN	—	—	—	—	—	—	—	Required	Required

* Third-party or vendor-specific WLAN security solutions that provide equivalent levels of authentication and encryption are acceptable.

** PDAs and other devices incapable of running personal firewall and antivirus software are exempt from this requirement.

- Agency reporting requirements.
  - ❑ Agencies shall report all 802.11 wireless LANs to the State Chief Information Officer.

ISO 17799: 2005 References
13.1.2 Reporting security weaknesses

090302 Cabling Security

Purpose: To provide an adequate level of confidentiality, integrity and availability for information sent via networks.

STANDARD

Agencies shall review the security of network cabling during upgrades or changes to hardware or facilities for signs of weak or missing physical security controls.

GUIDELINES

Agencies installing or maintaining telecommunication and/or power cabling should consider the following practices to increase the security and physical protection of the cabling:

- Underground cabling should be used, where possible, or lines with adequate alternative protection.
- Network cabling should be run through pipe or some other type of conduit and otherwise protected from possible damage.
- Power and communication cables should be segregated.
- Installers should be qualified to ensure that cabling complies with health, safety and building code requirements as appropriate.

RELATED INFORMATION

Standard 050206	Installing and Maintaining Network Cabling

ISO 17799: 2005 References
9.2.3 Cabling security

090303 Disaster Recovery Plan

Purpose: To maintain business continuity throughout the agency.

STANDARD

Agency management and information custodians must ensure that business continuity and disaster recovery plans are developed, maintained, tested on a prescribed basis and subjected to a continual update and improvement process.

RELATED INFORMATION

Standard 140101	Initiating the Business Continuity Planning Project
Standard 140102	Assessing the Business Continuity Plan Security Risk
Standard 140103	Developing the Business Continuity Plan
Standard 140104	Testing the Business Continuity Plan
Standard 140105 Continuity Plan	Training and Staff Awareness on the Business
Standard 140106	Maintaining and Updating the Business Continuity Plan

ISO 17799: 2005 References
14.1.3 Developing and implementing continuity plans including information security

HISTORY

State CIO Approval Date: March 22, 2006
Original Issue Date: March 22, 2006
Subsequent History:

Standard Number	Version	Date	Change/Description (Table Headings)

Old Security Policy/Standard	New Standard Numbers
Wireless Network Access Security Standard	090301 – Electronic Eavesdropping